

Département fédéral de l'intérieur DFI

Office fédéral de la statistique OFS
Division Infrastructure Statistique

Cahier des charges

- **Actualisation de la base de données du portefeuille informatique (budget, études, projets et applications) dans SAPxRPM Cockpit IKT**

- **Formation et support des chefs de projet concernant la saisie des rapports de projet dans SAPxRPM Cockpit IKT**

Neuchâtel, le 08 avril 2010

TABLE DES MATIERES

1. GENERALITES

But du document
L'objectif de ce document est de présenter les besoins spécifiques pour la mise à jour du portefeuille informatique et du budget informatique dans SAPxRPM Cockpit IKT ainsi que pour la formation et le support des chefs de projet de l'OFS dans l'application SAPxRPM Cockpit IKT, pour la partie IT du projet.

Ce document présente les conditions cadre pour l'appel d'offre, tenant compte des conditions générales de la Confédération relatives à l'achat de prestations informatiques et la procédure invitant à soumissionner.

2. SITUATION DE DEPART ET SITUATION EXISTANTE

Caractéristique du domaine spécialisé
L'Office de la Statistique dirige et coordonne le système de la statistique publique suisse. L'Office produit et publie des informations statistiques importantes sur l'état et l'évolution de la population, de l'économie, de la société, du territoire et de l'environnement.

Organisation
La section IT Management Support (ITMS) est responsable de la conduite de la stratégie informatique, le controlling IT, la sécurité informatique, le Provider-management ainsi que le conseil et le support des utilisateurs pour toutes les questions relatives à l'informatique.

Besoins
Jusqu'à présent, les chefs de projet ont établi un rapport de projet dans un document Word. Pour faciliter les analyses et centraliser les informations relatives aux projets, les rapports de projet et les budgets doivent être introduits dans SAPxRPM Cockpit IKT.

De plus, les informations de base des projets IT, le portefeuille informatique, sont stockées dans une base de données Access nommée InfoSys. La centralisation et l'actualisation de toutes les informations dans SAPxRPM Cockpit IKT fait partie de ce mandat.

Situation existante
Trois fois par année, les chefs de projet sont sollicités pour établir un rapport de projet. La plupart des projets sont constitués de deux parts interdépendantes : projet statistique et projet informatique. Les informations relatives au projet statistique sont saisies actuellement dans SAPxRPM par les chefs de projet. La partie informatique est décrite dans un document Word puis introduit partiellement et manuellement par le secrétariat de la division SI dans SAPxRPM Cockpit IKT.

Pour rationnaliser le processus, l'ensemble des informations relatives aux rapports de projet informatiques doivent être introduites par les chefs de projet dans SAPxRPM Cockpit IKT. Les données principales sont : base de données des projets, vue générale, délais, planification, statut du projet, description du projet, réalisation du projet, ressources financières, contrats en vigueur, analyse du risque, mesures pour réduire le risque, description de la situation actuelle, ressources en personnel, problèmes potentiels, prévisions et prochaines étapes.

3. DESCRIPTION DU PROJET ET PRESTATIONS A FOURNIR

Il est demandé à ce que la base de données des projets IT soit actualisée. Il s'agira de comparer InfoSys et SAPxRPM Cockpit IKT, de définir quelles sont les informations les plus actuelles et de mettre à jour les données dans SAPxRPM.

Les données financières relatives aux budgets 2010 et 2011 devront être complétées par le consultant externe et mises à jour par les chefs de projet dans la partie KNW de SAPxRPM.

Le projet vise à proposer une formation et un support aux chefs de projet de l'OFS pour qu'ils puissent saisir les rapports de projet et mettre à jour les budgets relatifs à leur projet IT dans SAPxRPM Cockpit IKT de manière indépendante et selon les Directives établies par l'Etat Major. La formation doit être dispensée en français et en allemand sur 2 x ½ journée dans chaque langue, le manuel d'utilisation rédigé en français et en allemand.

Suite à la formation, le prestataire de service se tient à disposition des chefs de projet pendant une durée déterminée. Il s'agit ici de donner la possibilité aux chefs de projet de soumettre leurs demandes et d'y répondre. Les questions et réponses doivent être reprises dans le manuel d'utilisation qui sera ainsi complété.

Les variantes relatives au type de support apporté aux chefs de projet après la formation doivent être décrites dans l'offre par le mandataire externe (conditions, nombre d'heures, types de prestations, présence sur site ou contact par téléphone, e-mail).

Il est nécessaire que l'intervenant externe connaisse parfaitement l'application SAPxRPM Cockpit IKT, la méthode ICO (surtout PCO) établie par l'IRB.

Nous estimons à 5 jours la mise à jour de la base de données SAPxRPM Cockpit IKT. La préparation de la formation aux chefs de projet, le cours et le support sont évalués à 5-10 jours. Au total, sont donc estimés **10-15 jours** de travail.

Planification
Les chefs de projet doivent établir leurs rapports de projet pour le 27 août 2010. Par conséquent, la planification suivante est applicable :

Mise à jour de la base de données : juin 2010
Formation : semaine 26 et semaine 33, année 2010
Soutien aux chefs de projets : semaines 33-35, année 2010

4. OBJECTIFS

Les objectifs suivants doivent être atteints par le mandataire jusqu'au 31 décembre 2010 :

- Les données de base du portefeuille informatique 2010 (études, projets, applications en cours) sont complètes et actualisées par le mandataire externe dans SAPxRPM
- Les budgets 2010 et 2011 des projets informatiques en cours ou planifiés sont saisis par le consultant externe dans SAPxRPM, KNW
- Les chefs de projets sont formés sur SAPxRPM Cockpit IKT et introduisent les rapports de projets qui les concernent dans le système de manière correcte et indépendante
- Le consultant externe fourni un support aux chefs de projet lors de la première saisie des rapports de projet informatiques dans SAPxRPM Cockpit IKT. Il est à disposition pour répondre aux questions éventuelles émanant des chefs de projet.

Dès 2011, les compétences acquises en 2010 permettront que :

- Les chefs de projets saisissent les rapports de projet dans SAPxRPM de manière correcte et indépendante
- Les collaborateurs de la section ITMS mettent à jour les données de base du portefeuille informatique (parties projets, études et applications)
- Les budgets 2011 et 2012 soient mis à jour par les chefs de projet

5. EXIGENCES

Critères d'évaluations

1. Avoir de très bonnes connaissances de SAPxRPM Cockpit IKT et de son utilisation au sein de l'administration fédérale. Le fournisseur de service doit pouvoir se prévaloir d'une expérience préalable similaire dans la formation sur SAPxRPM Cockpit IKT.

2. Maîtriser la méthode ICO (surtout PCO) définie par l'IRB

3. Fournir des prestations de qualité à un prix concurrentiel

4. Avoir de l'expérience dans la formation et dispenser la formation dans les locaux de l'OFS en deux langues : français et allemand. Etablir le support de cours « Manuel d'utilisation » en français et en allemand.
5. Se prévaloir d'une expérience confirmée dans la gestion de projet (description des projets similaires et fonction)

6. STRUCTURE DE L'OFFRE

Exigences envers le concept de solution
L'offre doit décrire précisément les prestations qui seront livrées (en tenant compte exactement des prestations à fournir selon cet appel d'offres) : description, nombre d'heures, taux horaire, nom du collaborateur et sa fonction, coût total. Le coût total doit être un montant plafonné qui englobe toutes les prestations et contient tous les frais accessoires à la réalisation du mandat : honoraires, charges sociales, frais, TVA (Les frais de déplacement ne sont pas facturables).

Une offre qui ne correspond pas précisément aux prestations à fournir selon cette demande d'offre ne sera pas considérée.

Le montant total de l'offre doit être en CHF et tenir compte de la TVA.

De plus, la société soumissionnaire doit présenter brièvement les projets similaires et démontrer que ses connaissances de l'application SAPxRPM Cockpit IKT sont adaptées au présent mandat.

Les différentes variantes de support apporté aux chefs de projet après la formation doivent être clairement décrites dans l'offre.

Structure de l'offre
La structure de l'offre est la suivante:

1. Brève présentation de la société soumissionnaire
2. Profil des collaborateurs (max 2 pages A4, formation, diplômes, projets, compétences)
3. Résumé de la prestation à l'intention de la direction
4. Solution proposée selon les critères du présent cahier des charges
5. Indications et commentaires relatifs aux exigences
6. Références : personnes de contact avec coordonnées de contact
7. Prix offert selon les dispositions de ce document
8. Informations complémentaires du soumissionnaire
9. Annexes

7. ASPECTS D'ORDRE ADMINISTRATIF

En envoyant une offre à l'OFS, l'entreprise soumissionnaire accepte que le contrat de prestations soit établit par l'OFS. Elle accepte que les conditions générales (de la Confédération) pour les prestations informatiques (édition de juin 1998), soient applicables aux prestations à fournir dans le domaine de la formation.

Ce document est à traiter de manière confidentielle. Le cahier des charges ne peut être utilisé à d'autres fins que celles nécessaires à l'établissement de l'offre. Le cahier des charges ainsi que toute documentation résultant de ce mandat reste propriété de l'Office Fédéral de la Statistique.

L'établissement de l'offre n'est pas rétribuée. L'offre peut être rédigée en français ou en allemand.

Les questions relatives au cahier des charges doivent être transmises jusqu'au **14 avril 2010, 12h00** à l'adresse e-mail suivante : ITinfo@bfs.admin.ch. Les réponses de l'OFS seront transmises par e-mail jusqu'au **19 avril 2010.**

L'offre doit être transmise jusqu'au **23 avril 2010** à l'adresse e-mail : ITinfo@bfs.admin.ch. Les offres reçues après ce délai ne seront pas prise en considération, la date de réception de l'e-mail fait foi.

L'offre doit avoir une validité de 60 jours au minimum.

Les offres seront évaluées selon les critères décrits dans le cahier des charges. La société choisie sera celle qui répondra le mieux aux critères. Le mandataire externe sera informé par l'OFS le **30 avril 2010.**

8. ANNEXES

Conditions générales (de la Confédération) pour les prestations informatiques (édition de juin 1998) http://www.bbl.admin.ch/bkb/00389/00398/00401/index.html?lang=fr

Règles d'utilisation des instruments des technologies de l'information et de la communication du Département fédéral de l'Intérieur version mars 2007.

Instructions relatives à l'utilisation des instruments des technologies de l'information et de la communication du Département Fédéral de l'Intérieur version mars 2007.

Documentation relative au Cockpit IKT (uniquement disponible en allemand) à adapter aux besoins de l'OFS : http://intranet.isb.admin.ch/themen/controlling/00790/01225/index.html?lang=de

Règles d'utilisation des instruments des technologies de l'information et de la communication

Les instruments des technologies de l'information et de la communication (instruments TIC) et les données du DFI qu'ils permettent de traiter doivent être protégés. En votre qualité d'utilisateurs de ces instruments, vous contribuerez à assurer cette protection en respectant les présentes règles. Les collaborateurs du DFI sont par ailleurs responsables, dans le cadre de leur travail, de la sécurité des données et des instruments TIC qui leur ont été confiés. Les présentes règles se basent sur les Instructions du DFI du 1er janvier 2005 concernant l'utilisation des instruments des technologies de l'information et de la communication.

- **Usage privé des TIC**
  L'usage privé est autorisé pour autant qu'il ne nuise pas au travail des collaborateurs, ne surcharge pas les instruments TIC du DFI et n'entraîne pas de risques pour la sécurité.

- **Courriels privés**
  Les courriels privés adressés à des destinataires internes ou externes doivent être munis du critère de diffusion «personnel».

- **Sauvegarde de données**
  Les données nécessaires aux tâches professionnelles doivent être sauvegardées dans les répertoires de groupes. Les données personnelles seront sauvegardées dans le répertoire personnel.

- **Mots de passe**
  Les mots de passe et autres procédés d'authentification (par ex. les cartes à puce) sont personnels et ne doivent pas être conservés dans un lieu librement accessible, ni notés en clair ou transmis à des tiers. Un mot de passe doit compter au moins huit signes et comporter des MAJUSCULES, des minuscules, des chiffres et des caractères spéciaux ($_!).

- **Transmission électronique d'informations dignes de protection**
  L'envoi d'informations confidentielles ou secrètes ou de données personnelles à des destinataires extérieurs à l'administration fédérale n'est autorisé que si les informations sont cryptées. Actuellement, le cryptage des données n'est pas encore possible partout pour des raisons techniques. Les collaborateurs sont priés d'en tenir compte et, le cas échéant, de renoncer à transmettre des données de ce genre par voie électronique.

- **Ordinateurs personnels**
  Les mécanismes de sécurité des ordinateurs situés à chaque poste de travail (antivirus par ex.)

ne doivent pas être désactivés ni modifiés. La mise à jour des logiciels antivirus et du système d'exploitation se fait automatiquement à chaque démarrage de l'ordinateur. Pour cette raison et pour des raisons écologiques, l'utilisateur doit arrêter son ordinateur chaque soir. Lorsqu'il quitte son bureau (pauses, séances), il doit s'assurer que personne d'autre que lui ne puisse utiliser son ordinateur. Il peut activer un économiseur d'écran protégé par un mot de passe ou fermer la porte de son bureau à clé.

- **Irrégularités relevant de la sécurité**
  Si les utilisateurs constatent sur les instruments TIC qu'ils utilisent ou gèrent des irrégularités relevant de la sécurité qui nécessitent une intervention urgente, un virus par exemple, ils doivent en informer immédiatement leur supérieur hiérarchique, le responsable de la sécurité informatique ou le Helpdesk.

- **Utilisation illicite**
  Est illicite toute utilisation des instruments TIC qui contrevient aux dispositions de la législation ou aux instructions concernant l'utilisation des technologies d'information et de communication. Il faut notamment respecter les dispositions ci-après du Code pénal suisse[1]:
  a) art. 135: Représentation de la violence
  b) art. 173-177: Diffamation
  c) art. 197: Pornographie
  d) art. 259: Provocation publique au crime ou à la violence
  e) art. 261: Atteinte à la liberté de croyance et des cultes
  f) art. 261bis: Discrimination raciale

- **Mesures en cas d'utilisation illicite**
  a) En cas d'utilisation illicite de TIC, le supérieur hiérarchique ou la direction de l'office peut décider que l'utilisateur concerné ne fera plus qu'un usage professionnel de certains instruments ou qu'il ne pourra plus du tout les utiliser.
  b) Selon la gravité de l'infraction, les mesures disciplinaires prévues par la législation sur le personnel s'appliquent. Sont réservées les exigences du Code civil. Ces mesures doivent respecter le principe de la proportionnalité.
  c) La poursuite pénale par les autorités judiciaires compétentes est réservée.

L'utilisateur confirme qu'il a pris connaissance des présentes règles et des instructions concernant l'utilisation des instruments des technologies d'informatique et de communication:

Date: Nom:

Signature:

Original aux services du personnel
Copie aux collaborateurs

---

[1] SR 311.0

Instructions relatives à l'utilisation des instruments des technologies de l'information et de la communication

Le Département fédéral de l'intérieur (DFI),

se fondant sur les lignes directrices concernant la sécurité informatique au DFI,
vu l'art. 8 de l'ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (OIAF) [1] et la loi du 19 juin 1992 sur la protection des données (LPD)[2],

émet les instructions ci-après:

Section 1: Objet, champ d'application, définitions

Art. 1 Objet
Les présentes instructions règlent l'utilisation des instruments des technologies de l'information et de la communication (TIC) au sein du Département fédéral de l'intérieur (DFI).

Art. 2 Champ d'application
Les présentes instructions sont valables pour les employés du DFI et ceux des entreprises partenaires ou externes qui ont accès aux instruments TIC du DFI.

Art. 3 Définitions
[1] Par instruments TIC, on entend tous les appareils, installations ou services qui servent au traitement, à la sauvegarde ou à la transmission électroniques d'informations, tels que ordinateurs, appareils périphériques, composants de réseau, logiciels, courriers électroniques (courriels), etc.
[2] Par informations, on entend les données et leur signification.
[3] Par données, on entend les informations sauvegardées physiquement qui se rapportent à des personnes ou à des choses.
[4] Par utilisateurs, on entend les employés du DFI et de ses entreprises partenaires qui se servent de ces instruments.

Section 2: Utilisation

Art. 4 Principes
[1] L'usage des instruments TIC est généralement réservé à l'accomplissement de tâches professionnelles. L'usage privé est autorisé pour autant qu'il ne nuise pas au travail des collaborateurs, ne surcharge pas lesdits instruments et n'entraîne pas de risques pour la sécurité.

---

[1] SR 172.010.58
[2] SR 235.1

[2] Les employés d'entreprises partenaires ou externes n'utilisent les instruments TIC du DFI que dans le cadre des mandats qui leur ont été confiés. Ils sont tenus par contrat de respecter les présentes instructions.
[3] Des dérogations justifiées à cette règle peuvent être accordées par le supérieur hiérarchique en accord avec le responsable de la sécurité informatique et le gestionnaire de l'intégration de l'office concerné. En cas de conflit, c'est la direction de l'office qui tranche. Les conditions de chaque dérogation doivent être fixées par écrit et signées par les parties concernées.

Art. 5 Utilisation illicite

[1] Est illicite toute utilisation des instruments TIC qui contrevient aux dispositions de l'ordonnance ou aux présentes instructions. Les dispositions ci-après du Code pénal suisse[3] doivent notamment être respectées:

a. art. 135: Représentation de la violence;
b. art. 173-177: Diffamation;
c. art. 197: Pornographie;
d. art. 259: Provocation publique au crime ou à la violence;
e. art. 261: Ateinte à la liberté de croyance et des cultes;
f. art. 261bis: Discrimination raciale

[2.] D'autres cas d'utilisation illicite sont recensés dans l'annexe aux présentes instructions.

Art. 6 Authentification

Les mots de passe et autres procédés d'authentification (par ex. les cartes à puce) sont strictement personnels et ne doivent pas être conservés dans un lieu librement accessible, notés en clair ni transmis à des tiers.

Art. 7 Communication externe

Les documents confidentiels ou classés secrets et les données personnelles ou particulièrement dignes de protection ne peuvent être envoyées à des destinataires extérieurs à l'administration fédérale via le réseau électronique de communication que si les conditions techniques de protection sont remplies (par ex. cryptage). Les utilisateurs sont priés d'en tenir compte et, le cas échéant, de renoncer à transmettre ce genre de données par voie électronique.

Art. 8 Courriels privés

Les courriels privés adressés à des destinataires internes ou externes doivent être munis du critère de diffusion «personnel». Le caractère privé du message peut ainsi être détecté avant de l'ouvrir. Si aucune distinction n'est faite entre message personnel et message professionnel et que les éléments de l'adresse ne permettent pas de reconnaître ou de déduire la nature privée du message, celui-ci est considéré comme un courrier professionnel.

Art. 9 Sauvegarde de données personnelles

Les collaborateurs sauvegardent leurs données personnelles exclusivement dans leur répertoire personnel. Les données nécessaires à l'accomplissement du travail professionnel doivent être sauvegardées dans les répertoires de données prévus à cet effet (par ex. dans les répertoires de groupe).

Art. 10 Mise à jour des ordinateurs personnels

La mise à jour des logiciels anti-virus et du système d'exploitation se fait automatiquement à chaque démarrage. L'utilisateur doit donc redémarrer chaque jour l'ordinateur de son poste de travail. Il doit par ailleurs l'éteindre chaque soir pour des raisons d'ordre écologique.

---

[3] SR 311.0

Art. 11 Durée d’utilisation
Les instruments TIC mis à la disposition des collaborateurs par le département ne doivent plus être utilisés après la cessation des rapports de travail. S’il en avait fourni à des entreprises partenaires, elles doivent les restituer une fois leur mandat achevé.

Section 3: Mesures pour l’application des instructions

Art. 12 Contrôle
[1] Le contrôle de l’application des présentes instructions incombe au supérieur hiérarchique, pour autant que les dispositions ci-après ne prévoient rien d’autre.
[2] Si des utilisateurs constatent une utilisation abusive des instruments TIC, ils doivent en informer leur supérieur hiérarchique, le responsable de la sécurité informatique ou la direction de l’office.
[3] Si les utilisateurs constatent dans le domaine de la sécurité des irrégularités nécessitant une intervention urgente, par exemple un virus, ils doivent en informer immédiatement leur supérieur hiérarchique, le responsable de la sécurité informatique ou le Helpdesk.

Art. 13 Dispositifs de sécurité techniques
Pour éviter toute utilisation illicite des instruments TIC, il est possible d’installer des dispositifs de sécurité technique, comme des pare-feu, des diskquotas ou des barrages à certains sites Internet par exemple.

Art. 14 Protocole des accès
[1] L’utilisation des instruments TIC est consignée dans un protocole de façon anonyme ou pseudo-anonyme. Les collaborateurs sont informés des protocoles les concernant.
[2] Si des contrôles anonymes révèlent que les prescriptions légales ou les présentes directives ne sont pas respectées, il faut rendre les collaborateurs attentifs au fait que ces activités doivent cesser. Ce n’est qu’ensuite que des lectures de protocole ou des contrôles détaillés peuvent être entrepris pour identifier les fautifs.
[3] Le contrôle portant sur une personne déterminée doit être effectué selon le principe «des quatre yeux» (double contrôle). Il ne peut avoir lieu que si la direction de l’office en a donné l’ordre.

Art. 15 Mesures en cas d’utilisation illicite
[1] En cas d’utilisation illicite d’instruments TIC, le supérieur hiérarchique ou la direction de l’office peut décider que l’utilisateur concerné ne fera plus qu’un usage professionnel de certaines technologies ou qu’il ne pourra plus du tout les utiliser.
[2] Selon la gravité de l’infraction, les mesures disciplinaires prévues dans la législation sur le personnel s’appliquent. Restent réservées les exigences du Code civil. Ces mesures doivent respecter le principe de la proportionnalité.
[3] La poursuite pénale par les autorités judiciaires compétentes reste réservée.

Section 4: Dispositions finales

Les présentes instructions entrent en vigueur le 1er janvier 2005.

DÉPARTEMENT FÉDÉRAL DE L'INTÉRIEUR
Le secrétaire général

Pascal Strupler

Annexe: Utilisation illicite, compléments à l'art. 5

[1] Sont illicites les actions suivantes:

a. copier, installer, utiliser ou diffuser des logiciels, des données et des informations en tout genre comme des systèmes d'exploitation, des logiciels de bureautique, de la musique, des films ou des livres, s'ils sont protégés par des droits d'auteur;
b. élaborer ou diffuser des programmes dangereux comme des virus ou des chevaux de Troie;
c. utiliser de faux renseignements informatiques (spoofing), par exemple des adresses IP, des adresses MAC;
d. envoyer des courriels en donnant une fausse adresse d'expéditeur;
e. envoyer des SPAM.

[2] Sont également considérées comme utilisation illicite les actions qui mettent en péril la sécurité comme:

a. mettre hors circuit ou contourner les mécanismes de sécurité installés sur les ordinateurs, comme les logiciels anti-virus et les pare-feu;
b. quitter son poste de travail sans verrouiller l'accès à l'ordinateur ou se déconnecter;
c. installer ou utiliser des instruments TIC étrangers à l'intérieur du réseau du DFI, par exemple en connectant un ordinateur portable privé au réseau interne;
d. mettre les instruments TIC à disposition de tiers non habilités à les utiliser;
e. installer et utiliser sans autorisation des connexions entre le réseau interne de la Confédération (réseau «bleu» de l'administration fédérale) et des réseaux externes (Internet), par exemple au moyen de Wireless-LAN ou Bluetooth;
f. surcharger les systèmes informatiques et de communication en faisant passer de grandes quantités de données par Intranet, par exemple des fichiers de musique MP3, des vidéos ou des logiciels téléchargés.

Formatiert: Nummerierung und Aufzählungszeichen

[3] Sont interdites en outre les actions relevant du piratage (hacking, cracking), par exemple:

a. entrer ou essayer d'entrer dans des systèmes d'ordinateurs étrangers ou des comptes d'utilisateurs étrangers, même en l'absence de mesures de protection explicites;
b. perturber l'exploitation d'ordinateurs ou de réseaux, par ex. par des attaques du genre «Déni de service»;
c. fouiller sans autorisation des ordinateurs ou des réseaux internes ou externes, par exemple par port-scanning ou sniffing;
d. se livrer à l'espionnage pour obtenir des mots de passe.

Annexe: glossaire

Hacking / cracking
Un hacker ou mordu était à l'origine un programmateur ou un administrateur de système doué qui possédait des connaissances exceptionnelles du matériel et des logiciels. Il utilisait ces connaissances pour améliorer les systèmes d'ordinateur. Le cracker ou pirate dispose la plupart du temps de capacités égales à celles du hacker, mais les emploie pour s'introduire dans des systèmes étrangers dans l'intention de nuire.

Attaques Denial of Service
Une attaque de déni de service (Denial of Service; DoS) a pour but de mettre certains programmes ou tout le système d'un ordinateur hors service. Techniquement, il se passe ceci: un serveur est bombardé de demandes à tel point que le système, débordé, ne peut plus remplir toutes les tâches demandées. Dans le pire des cas, il s'effondre.

Port-Scanning
Un attaquant tente de trouver quels sont les services offerts par un centre de calcul en les activant tous les uns après les autres. Un port-scan sert en général à préparer une attaque.

Spoofing
Ici, l'expéditeur se présente au destinataire du message sous une fausse identité. Pour cela, il change l'adresse IP ou MAC de son ordinateur.

Sniffing
Il s'agit d'espionnage par écoute du trafic de données à l'intérieur du réseau. Un sniffer est un programme qui enregistre tous les paquets de données d'un segment du réseau et qui parvient ainsi à espionner notamment les mots de passe et les données.

SPAM
Terme général qui désigne les envois en masse de courriels indésirables. Le «spamming» peut être comparé aux envois publicitaires non adressés ou au démarchage par appels téléphoniques ou par fax.